The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Andreas Gohr -- DokuWiki	The spellchecker (spellcheck.php) in DokuWiki 2006/06/04 and earlier allows remote attackers to insert and execute arbitrary PHP code via "complex curly syntax" that is inserted into a regular expression that is processed by preg_replace with the /e (executable) modifier.	unknown 2006-06-06	7.0	CVE-2006-2878 OTHER-REF OTHER-REF SECUNIA BUGTRAQ BID FRSIRT SECTRACK
Aspburst -- myNewsletter	Multiple SQL injection vulnerabilities in myNewsletter 1.1.2 and earlier allow remote attackers to execute arbitrary SQL commands via the UserName parameter in (1) validatelogin.asp or (2) adminlogin.asp.	2006-06-05 2006-06-07	7.0	CVE-2006-2887 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA
AssoCIateD -- AssoCIateD CMS	Multiple PHP remote file inclusion vulnerabilities in AssoCIateD (aka ACID) CMS 1.1.3 allow remote attackers to execute arbitrary PHP code via a URL in the root_path parameter to (1) menu.php, (2) profile.php, (3) users.php, (4) cache_mngt.php, and (5) gallery_functions.php.	2006-06-01 2006-06-06	7.0	CVE-2006-2841 Milw0rm BID OTHER-REF FRSIRT SECUNIA
Bookmark4U -- Bookmark4U	PHP remote file inclusion vulnerability in Bookmark4U 2.0.0 and earlier allows remote attackers to include arbitrary PHP files via the include_prefix parameter in (1) inc/dbase.php, (2) inc/config.php, (3) inc/common.php, and (4) inc/function.php. NOTE: it has been reported that the inc directory is protected by a .htaccess file, so this issue only applies in certain environments or configurations.	unknown 2006-06-06	7.0	CVE-2006-2877 BUGTRAQ BUGTRAQ BID SECTRACK
CoolForum -- CoolForum	SQL injection vulnerability in editpost.php in CoolForum 0.8.3 beta and earlier allows remote attackers to execute arbitrary SQL commands via the post parameter.	unknown 2006-06-06	7.0	CVE-2006-2867 BUGTRAQ OTHER-REF SECTRACK BID
Cyboards -- Cyboards PHP Lite	PHP remote file inclusion vulnerability in include/common.php in CyBoards PHP Lite 1.25 allows remote attackers to execute arbitrary PHP code via a URL in the script_path parameter.	unknown 2006-06-06	7.0	CVE-2006-2871 BUGTRAQ BID
DeltaScripts -- PHP ManualMaker	Multiple cross-site scripting (XSS) vulnerabilities in PHP ManualMaker 1.0 allows remote attackers to inject arbitrary web script or HTML via the (1) id parameter to index.php, (2) search field (possibly the s parameter), or (3) comment field.	2006-06-02 2006-06-03	7.0	CVE-2006-2803 BUGTRAQ BID FRSIRT SECUNIA
DeltaScripts -- Pro Publish	Cross-site scripting (XSS) vulnerability in cat.php in PHP Pro Publish 2.0 allows remote attackers to inject arbitrary web script or HTML via the catname parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-06-06	7.0	CVE-2006-2876 FRSIRT SECUNIA
Dreamcost -- DreamAccount	Multiple PHP remote file inclusion vulnerabilities in DreamAccount 3.1 and earlier, when register_globals is enabled, allow remote attackers to execute arbitrary PHP code via a URL in the da_path parameter in the (1) auth.cookie.inc.php, (2) auth.header.inc.php, or (3) auth.sessions.inc.php	unknown 2006-06-07	7.0	CVE-2006-2881 BUGTRAQ BUGTRAQ OTHER-REF

	scripts.			OTHER-REF BID FRSIRT SECUNIA XF
Drupal -- Drupal	Drupal 4.6.x before 4.6.8 and 4.7.x before 4.7.2, when running under certain Apache configurations such as when FileInfo overrides are disabled within .htaccess, allows remote attackers to execute arbitrary code by uploading a file with multiple extensions, a variant of CVE-2006-2743.	unknown 2006-06-05	7.0	CVE-2006-2831 BUGTRAQ OTHER-REF OTHER-REF BID
Full Revolution -- aspWebLinks	links.asp in aspWebLinks 2.0 allows remote attackers to change the administrative password, possibly via a direct request with a modified txtAdministrativePassword field.	2006-06-01 2006-06-06	7.0	CVE-2006-2848 BUGTRAQ OTHER-REF
gnopaste -- gnopaste	PHP remote file inclusion vulnerability in includes/common.php in gnopaste 0.5.3 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the root_path parameter.	unknown 2006-06-06	7.0	CVE-2006-2834 OTHER-REF OTHER-REF BID OTHER-REF FRSIRT SECTRACK
Goss -- iCM	Cross-site scripting (XSS) vulnerability in index.cfm in Goss Intelligent Content Management (iCM) 7.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the keyword parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party sources.	unknown 2006-06-03	7.0	CVE-2006-2804 BID FRSIRT SECUNIA
HP -- Tru64 UNIX HP -- Internet Express	Unspecified vulnerability in HP Tru64 UNIX 4.0F PK8 up to 5.1B-3 and HP Internet Express for Tru64 UNIX 6.3 through 6.5, when running Sendmail, might allow remote attackers to cause a denial of service or execute arbitrary code. NOTE: as of 20060607, due to the lack of details, it is not publicly known whether this issue is within Sendmail itself, and/or if it is specific to HP.	unknown 2006-06-07	7.0	CVE-2006-1173 HP CERT-VN SECUNIA FRSIRT
libTIFF -- libTIFF	Buffer overflow in the t2p_write_pdf_string function in tiff2pdf in libtiff 3.8.2 and earlier allows attackers to cause a denial of service (crash) and possibly execute arbitrary code via a TIFF file with a DocumentName tag that contains UTF-8 characters, which triggers the overflow when a character is sign extended to an integer that produces more digits than expected in an sprintf call.	2006-05-10 2006-06-08	7.0	CVE-2006-2193 DEBIAN BUGZILLA DEBIAN FRSIRT SECUNIA UBUNTU SECUNIA SECUNIA
LoudHush -- LoudHush	Unspecified vulnerability in the iaxclient library LoudHush 1.3.6 has unknown impact and remote attack vectors.	unknown 2006-06-09	7.0	CVE-2006-2923 OTHER-REF BID SECUNIA
Mozilla -- Firefox Mozilla -- Thunderbird	Mozilla Firefox and Thunderbird before 1.5.0.4 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via (1) nested tags in a select tag, (2) a DOMNodeRemoved mutation event, (3) "Content-implemented tree views," (4) BoxObjects, (5) the XBL implementation, (6) an iframe that attempts to remove itself, which leads to memory corruption.	unknown 2006-06-02	7.0	CVE-2006-2779 OTHER-REF CERT-VN CERT BUGTRAQ BID FRSIRT SECTRACK SECTRACK SECUNIA SECUNIA
OpenEMR -- OpenEMR	PHP remote file inclusion vulnerability in contrib/forms/evaluation/C_FormEvaluation.class.php in OpenEMR 2.8.1 and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the GLOBALS[fileroot] parameter.	unknown 2006-06-09	7.0	CVE-2006-2929 OTHER-REF FRSIRT SECUNIA
Out of the Trees Web Design -- SelectaPix	Multiple SQL injection vulnerabilities in SelectaPix 1.31 allow remote attackers to execute arbitrary SQL commands via the (1) albumID parameter to (a) view_album.php or (b) index.php, (2) imageID parameter to (c) popup.php, or (3) username and (4) password parameters to (d) admin/member.php.	unknown 2006-06-09	7.0	CVE-2006-2912 OTHER-REF SECUNIA
Particle Software -- Particle Links	SQL injection vulnerability in index.php in Partial Links 1.2.2 allows remote attackers to execute arbitrary SQL commands via the topic parameter.	unknown 2006-06-08	7.0	CVE-2006-2904 BUGTRAQ SECUNIA

phpBB Group -- phpBB	** DISPUTED ** PHP remote file inclusion vulnerability in template.php in phpBB 2 allows remote attackers to execute arbitrary PHP code via a URL in the page parameter. NOTE: followup posts have disputed this issue, stating that template.php does not appear in phpBB and does not use a $page variable. It is possible that this is a site-specific vulnerability, or an issue in a mod.	2006-06-03 2006-06-06	7.0	CVE-2006-2865 BUGTRAQ BUGTRAQ BUGTRAQ BID BUGTRAQ
PmWiki -- PmWiki	Cross-site scripting (XSS) vulnerability in (1) uploads.php and (2) "url links" in PmWiki 2.1.6 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified parameters.	unknown 2006-06-06	7.0	CVE-2006-2840 OTHER-REF FRSIRT SECUNIA
PyBlosxom -- PyBlosxom	Cross-site scripting (XSS) vulnerability in the Contributed Packages for PyBlosxom 1.2.2 and earlier allows remote attackers to inject arbitrary web script or HTML via the Comments plugin in the (1) url and (2) author fields.	unknown 2006-06-07	7.0	CVE-2006-2880 SOURCEFORGE FRSIRT SECUNIA BID
Qbik -- WinGate	Stack-based buffer overflow in the WWW Proxy Server of Qbik WinGate 6.1.1.1077 allows remote attackers to cause a denial of service and possibly execute arbitrary code via a long URL HTTP request.	unknown 2006-06-09	7.0	CVE-2006-2926 FULLDISC FULLDISC FRSIRT SECUNIA
QontentOne -- QontentOne CMS	Cross-site scripting (XSS) vulnerability in search.php in QontentOne CMS allows remote attackers to inject arbitrary web script or HTML via the search_phrase parameter.	unknown 2006-06-02	7.0	CVE-2006-2774 BID FRSIRT SECUNIA BUGTRAQ BUGTRAQ SECTRACK XF
Rumble -- Rumble	PHP remote file inclusion vulnerability in config.php in Rumble 1.02 allows remote attackers to execute arbitrary PHP code via a URL in the configArr[pathtodir] parameter.	unknown 2006-06-06	7.0	CVE-2006-2872 BUGTRAQ MLIST MLIST
SquirrelMail -- SquirrelMail	** DISPUTED ** PHP remote file inclusion vulnerability in functions/plugin.php in SquirrelMail 1.4.6 and earlier, if register_globals is enabled and magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary PHP code via a URL in the plugins array parameter. NOTE: this issue has been disputed by third parties, who state that Squirrelmail provides prominent warnings to the administrator when register_globals is enabled. Since the varieties of administrator negligence are uncountable, perhaps this type of issue should not should not be included in CVE. However, the original developer has posted a security advisory, so there might be relevant real-world environments under which this vulnerability is applicable.	2006-06-01 2006-06-06	7.0	CVE-2006-2842 BUGTRAQ OTHER-REF SQUIRRELMAIL FRSIRT SECUNIA BID SECTRACK
Tibco -- Hawk Monitoring Agent Tibco -- Runtime Agent Tibco -- Hawk	Buffer overflow in Hawk Monitoring Agent (HMA) for TIBCO Hawk before 4.6.1 and TIBCO Runtime Agent (TRA) before 5.4 allows authenticated users to execute arbitrary code via the configuration for tibhawkhma.	2006-06-05 2006-06-05	7.0	CVE-2006-2829 OTHER-REF CERT-VN BID FRSIRT SECUNIA
Two Shoes Mambo Factory -- SimpleBoard	Multiple cross-site scripting (XSS) vulnerabilities in Two Shoes M-Factory (TSMF) SimpleBoard 1.1.0 Stable (aka com_simpleboard), as used in Mambo and Joomla!, allow remote attackers to inject arbitrary web script or HTML via (1) the Name field in "post ne topic" in the Frontend, (2) the Title (aka Community-Title) field in Simpleboard Configuration in the Backend Admin Panel, and the (3) Name (aka Forum-Title) and (4) Name (aka Category-Title) fields in Simpleboard Administration in the Backend Admin Panel. NOTE: some sources have stated that the sb_authorname parameter is affected, but it is unclear which field is related to it.	2006-06-01 2006-06-05	7.0	CVE-2006-2815 BUGTRAQ FULLDISC BID FRSIRT SECUNIA
Wikiwig -- Wikiwig	PHP remote file inclusion vulnerability in _wk/wk_lang.php in Wikiwig 4.1 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the WK[wkPath] parameter.	2006-06-06 2006-06-07	7.0	CVE-2006-2888 OTHER-REF BID FRSIRT SECUNIA

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info

Abarcar Software -- Abarcar Realty Portal	SQL injection vulnerability in content.php in abarcar Realty Portal 5.1.5 allows remote attackers to execute arbitrary SQL commands via the cat parameter.	2006-06-01 2006-06-06	4.7	CVE-2006-2853 OTHER-REF BID OTHER-REF FRSIRT SECUNIA
ALWIL -- Avast! Antivirus	Unspecified vulnerability in the CHM unpacker in avast! before 4.7.844 has unknown impact and remote attack vectors.	unknown 2006-06-06	4.9	CVE-2006-2869 OTHER-REF BID FRSIRT SECUNIA
Andrew Godwin -- ByteHoard	PHP remote file inclusion vulnerability in includes/webdav/server.php in Bytehoard 2.1 Epsilon/Delta allows remote attackers to execute arbitrary PHP code via a URL in the bhconfig[bhfilepath] parameter.	2006-06-02 2006-06-06	4.7	CVE-2006-2849 OTHER-REF SECUNIA BUGTRAQ BID FRSIRT SECTRACK OSVDB
Apache Software Foundation -- SpamAssassin	SpamAssassin before 3.1.3, when running with vpopmail and the paranoid (-P) switch, allows remote attackers to execute arbitrary commands via a crafted message that is not properly handled when invoking spamd with the virtual pop username.	unknown 2006-06-06	5.6	CVE-2006-2447 OTHER-REF DEBIAN REDHAT BID FRSIRT SECUNIA SECUNIA BUGTRAQ SECUNIA
Arabless -- SaphpLesson	SQL injection vulnerability in saphplesson 2.0 allows remote attackers to execute arbitrary SQL commands via the (1) forumid parameter in add.php and (2) lessid parameter in show.php.	unknown 2006-06-06	4.9	CVE-2006-2835 BUGTRAQ
ASPScriptz -- ASPScriptz Guest Book	Multiple cross-site scripting (XSS) vulnerabilities submit.asp in ASPScriptz Guest Book 2.0 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) GBOOK_UNAME, (2) GBOOK_EMAIL, (3) GBOOK_CITY, (4) GBOOK_COU, (5) GBOOK_WWW, and (6) GBOOK_MESS form fields.	2006-05-18 2006-06-07	4.7	CVE-2006-2882 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA
BlueShoes -- BlueShoes Framework	Multiple PHP remote file inclusion vulnerabilities in BlueShoes Framework 4.6 allow remote attackers to execute arbitrary PHP code via a URL in the (1) APP[path][applications] parameter to (a) Bs_Faq.class.php, (2) APP[path][core] parameter to (b) fileBrowserInner.php, (c) file.php, and (d) viewer.php, and (e) Bs_ImageArchive.class.php, (3) GLOBALS[APP][path][core] parameter to (f) Bs_Ml_User.class.php, or (4) APP[path][plugins] parameter to (g) Bs_Wse_Profile.class.php.	2006-06-03 2006-06-06	5.6	CVE-2006-2864 Milw0rm BID FRSIRT SECUNIA
Claroline -- Claroline	Multiple PHP remote file inclusion vulnerabilities in Claroline 1.7.6 allow remote attackers to execute arbitrary PHP code via a URL in the includePath cookie to (1) auth/extauth/drivers/mambo.inc.php or (2) auth/extauth/drivers/postnuke.inc.php.	unknown 2006-06-06	5.6	CVE-2006-2868 OTHER-REF FRSIRT SECUNIA BID
CMPro Team -- Clan Manager Pro	PHP remote file inclusion vulnerability in cmpro_header.inc.php in Clan Manager Pro (CMPRO) 1.1 and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the (1) cm_ext_server and (2) sitepath parameters.	unknown 2006-06-09	5.6	CVE-2006-2921 OTHER-REF FRSIRT SECUNIA
CMS-Bandits -- CMS-Bandits	Multiple PHP remote file inclusion vulnerabilities in CMS-Bandits 2.5 and earlier, when register_globals is enabled, allow remote attackers to execute arbitrary PHP code via a URL in the spaw_root parameter in (1) dialogs/img.php and (2) dialogs/td.php.	unknown 2006-06-09	5.6	CVE-2006-2928 BUGTRAQ FRSIRT SECUNIA
CS-Cart -- CS-Cart	PHP remote file inclusion vulnerability in class.cs_phpmailer.php in CS-Cart 1.3.3 allows remote attackers to execute arbitrary PHP code via a URL in the classes_dir parameter.	2006-06-03 2006-06-06	5.6	CVE-2006-2863 Milw0rm BID FRSIRT SECUNIA
Dotclear -- Dotclear	PHP remote file inclusion vulnerability in layout/prepend.php in DotClear 1.2.4 and earlier allows remote attackers to execute arbitrary PHP code via a FTP URL in the blog_dc_path parameter, which passes file_exists() and is_dir() tests on PHP 5.	unknown 2006-06-06	5.6	CVE-2006-2866 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA

Dotproject -- Dotproject	Cross-site scripting (XSS) vulnerability in index.php in dotProject 2.0.2 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified parameters, which are not properly handled when the client is using Internet Explorer.	2006-06-05 2006-06-06	4.7	CVE-2006-2851 OTHER-REF OTHER-REF FRSIRT SECUNIA BID
dotWidget -- dotWidget CMS	PHP remote file inclusion vulnerability in dotWidget CMS 1.0.6 and earlier, when register_globals is enabled, allowd remote attackers to execute arbitrary PHP code via a URL in the file_path parameter in (1) index.php, (2) feedback.php, and (3) printfriendly.php.	2006-06-02 2006-06-06	4.7	CVE-2006-2852 BUGTRAQ OTHER-REF BID SECUNIA FRSIRT SECTRACK
ESTsoft -- InternetDISK	Unspecified vulnerability in ESTsoft InternetDISK versions before 2006/04/20 allows remote authenticated users to execute arbitrary code, possibly by uploading a file with multiple extensions into the WebLink directory.	2006-04-19 2006-06-07	4.2	CVE-2006-2899 BUGTRAQ BID
F-Secure -- Anti-Virus F-Secure -- Internet Gatekeeper	Buffer overflow in the web console in F-Secure Anti-Virus for Microsoft Exchange 6.40, and Internet Gatekeeper 6.40 through 6.42 and 6.50 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unknown attack vectors. NOTE: By default, the connections are only allowed from the local host.	unknown 2006-06-06	4.7	CVE-2006-2838 OTHER-REF FRSIRT SECUNIA SECTRACK SECTRACK
Full Revolution -- aspWebLinks	SQL injection vulnerability in links.asp in aspWebLinks 2.0 allows remote attackers to execute arbitrary SQL commands via the linkID parameter.	2006-06-02 2006-06-06	4.7	CVE-2006-2847 BUGTRAQ OTHER-REF SECUNIA BID FRSIRT
iBWd -- iBWd Guestbook	SQL injection vulnerability in index.php in iBWd Guestbook 1.0 allows remote attackers to execute arbitrary SQL commands via the offset parameter.	2006-06-03 2006-06-06	4.7	CVE-2006-2854 OTHER-REF BID FRSIRT SECUNIA
KKE Info Media -- Kmita FAQ	Cross-site scripting (XSS) vulnerability in search.php in Kmita FAQ 1.0 allows remote attackers to inject arbitrary web script or HTML via the q parameter.	2006-06-05 2006-06-07	4.7	CVE-2006-2883 BUGTRAQ BID SECUNIA FRSIRT
KKE Info Media -- Kmita FAQ	SQL injection vulnerability in index.php in Kmita FAQ 1.0 allows remote attackers to execute arbitrary SQL commands via the catid parameter.	2006-06-05 2006-06-07	4.7	CVE-2006-2884 BUGTRAQ BID SECUNIA FRSIRT
knowledgetree -- knowledgetree	Multiple cross-site scripting (XSS) vulnerabilities in KnowledgeTree Open Source 3.0.3 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) fDocumentId parameter in view.php and the (2) fSearchableText parameter in /search/simpleSearch.php.	2006-06-06 2006-06-07	4.7	CVE-2006-2885 OTHER-REF FRSIRT SECUNIA BID
Lifetype -- Lifetype	SQL injection vulnerability in index.php in LifeType 1.0.4 allows remote attackers to execute arbitrary SQL commands via the articleId parameter in a ViewArticle action (viewarticleaction.class.php).	2006-06-05 2006-06-06	4.7	CVE-2006-2857 BUGTRAQ OTHER-REF BID SECUNIA FRSIRT
Locazo! -- LocazoList Classifieds	SQL injection vulnerability in viewmsg.asp in LocazoList Classifieds 1.05e allows remote attackers to execute arbitrary SQL commands via the msgid parameter.	2006-06-02 2006-06-06	4.7	CVE-2006-2858 BUGTRAQ BID BUGTRAQ FRSIRT SECTRACK SECUNIA
Miraks -- MiraksGalerie	Multiple PHP remote file inclusion vulnerabilities in MiraksGalerie 2.62 allow remote attackers to execute arbitrary PHP code via a URL in the (1) g_pcltar_lib_dir parameter in (a) pcltar.lib.php when register_globals is enabled, and (2) listconfigfile[] parameter in (b) galsecurity.lib.php and (c) galimage.lib.php.	unknown 2006-06-09	5.6	CVE-2006-2922 BUGTRAQ SECUNIA

myWebland -- myBloggie	** DISPUTED ** PHP remote file inclusion vulnerability in MyBloggie 2.1.1 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the mybloggie_root_path parameter to (1) admin.php or (2) scode.php. NOTE: this issue has been disputed in multiple third party followups, which say that the MyBloggie source code does not demonstrate the issue, so it might be the result of another module. CVE analysis as of 20060605 agrees with the dispute. In addition, scode.php is not part of the MyBloggie distribution.	2006-06-02 2006-06-06	4.7	CVE-2006-2859 BUGTRAQ BUGTRAQ BID BUGTRAQ
Ottoman -- Ottoman	PHP remote file inclusion vulnerability in Ottoman 1.1.2, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via the default_path parameter in (1) error.php, (2) index.php, and (3) classes/main_class.php.	unknown 2006-06-02	5.6	CVE-2006-2767 OTHER-REF BID FRSIRT SECUNIA OSVDB OSVDB
Particle Soft -- Particle Wiki	SQL injection vulnerability in index.php in Particle Wiki 1.0.2 and earlier allows remote attackers to execute arbitrary SQL commands via the version parameter.	2006-06-05 2006-06-06	4.7	CVE-2006-2861 OTHER-REF FRSIRT SECUNIA BID
Particle Soft -- Particle Gallery	SQL injection vulnerability in viewimage.php in Particle Gallery 1.0.0 and earlier allows remote attackers to execute arbitrary SQL commands via the imageid parameter.	2006-06-05 2006-06-06	4.7	CVE-2006-2862 OTHER-REF FRSIRT SECUNIA BID
PHP Labware -- LabWiki	Cross-site scripting (XSS) vulnerability in recentchanges.php in PHP Labware LabWiki 1.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the help parameter.	2006-06-05 2006-06-06	4.7	CVE-2006-2850 OTHER-REF FRSIRT SECUNIA BID
Pineapple Technologies -- Lore	SQL injection vulnerability in comment.php in Pineapple Technologies Lore 1.5.6 and earlier allows remote attackers to execute arbitrary SQL commands via the article_id parameter.	unknown 2006-06-06	4.9	CVE-2006-2836 OTHER-REF FRSIRT SECUNIA
Pixelpost -- Pixelpost	Multiple SQL injection vulnerabilities in index.php in Pixelpost 1-5rc1-2 and earlier allow remote attackers to execute arbitrary SQL commands, and leverage them to gain administrator privileges, via the (1) category or (2) archivedate parameter.	unknown 2006-06-07	5.6	CVE-2006-2889 BUGTRAQ OTHER-REF BID SECTRACK
Pixelpost -- Pixelpost	Pixelpost 1-5rc1-2 and earlier, when register_globals is enabled, allows remote attackers to gain administrator privileges and conduct other attacks by setting the _SESSION["pixelpost_admin"] parameter to 1 in calls to admin scripts such as admin/view_info.php.	unknown 2006-06-07	5.6	CVE-2006-2890 BUGTRAQ OTHER-REF BID SECTRACK
Redaxo -- Redaxo	PHP remote file inclusion vulnerability in Redaxo 2.7.4 allows remote attackers to execute arbitrary PHP code via a URL in the (1) REX[INCLUDE_PATH] parameter in (a) addons/import_export/pages/index.inc.php and (b) pages/community.inc.php.	2006-06-02 2006-06-06	4.7	CVE-2006-2843 BUGTRAQ OTHER-REF SECUNIA FRSIRT SECTRACK
Redaxo -- Redaxo	Multiple PHP remote file inclusion vulnerabilities in Redaxo 3.0 allow remote attackers to execute arbitrary PHP code via a URL in the REX[INCLUDE_PATH] parameter to (1) simple_user/pages/index.inc.php and (2) stats/pages/index.inc.php.	2006-06-02 2006-06-06	4.7	CVE-2006-2844 BUGTRAQ OTHER-REF SECUNIA FRSIRT SECTRACK
Redaxo -- Redaxo	PHP remote file inclusion vulnerability in Redaxo 3.0 up to 3.2 allows remote attackers to execute arbitrary PHP code via a URL in the REX[INCLUDE_PATH] parameter to image_resize/pages/index.inc.php.	2006-06-02 2006-06-06	4.7	CVE-2006-2845 BUGTRAQ OTHER-REF SECUNIA FRSIRT SECTRACK
Sun -- Sun Grid Engine Sun -- Sun N1 Grid Engine	Unspecified vulnerability in Sun Grid Engine 5.3 and Sun N1 Grid Engine 6.0, when configured in Certificate Security Protocol (CSP) Mode, allows local users to shut down the grid service or gain access, even if access is denied.	unknown 2006-06-09	4.9	CVE-2006-2930 SUNALERT FRSIRT SECUNIA
VisionGate -- VisionGate Portal System	Cross-site scripting (XSS) vulnerability in Print.PHP in VisionGate Portal System allows remote attackers to inject arbitrary web script or HTML via unspecified parameters. NOTE: The provenance of this information is unknown; the details are obtained solely from third party information.	2006-06-01 2006-06-06	4.7	CVE-2006-2846 BID

Webspot -- WebspotBlogging	PHP remote file inclusion vulnerability in Webspotblogging 3.0.1 allows remote attackers to execute arbitrary PHP code via a URL in the path parameter to (1) inc/logincheck.inc.php, (2) inc/adminheader.inc.php, (3) inc/global.php, or (4) inc/mainheader.inc.php.	2006-06-03 2006-06-06	4.7	CVE-2006-2860 OTHER-REF BID SECUNIA FRSIRT
xueBook -- xueBook	SQL injection vulnerability in index.php in xueBook 1.0 allows remote attackers to execute arbitrary SQL commands via the start parameter.	2006-06-03 2006-06-06	4.7	CVE-2006-2855 OTHER-REF BID FRSIRT SECUNIA

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Activestate -- ActivePerl	ActiveState ActivePerl 5.8.8.817 for Windows configures the site/lib directory with "Users" group permissions for changing files, which allows local users to gain privileges by creating a malicious sitecustomize.pl file in that directory. NOTE: The provenance of this information is unknown; the details are obtained solely from third party information.	2006-06-05 2006-06-06	3.3	CVE-2006-2856 SECUNIA BID FRSIRT
Alex -- News-Engine	SQL injection vulnerability in newscomments.php in Alex News-Engine 1.5.0 and earlier allows remote attackers to execute arbitrary SQL commands via the newsid parameter.	unknown 2006-06-07	2.3	CVE-2006-2879 BUGTRAQ BID FRSIRT SECUNIA
Asterisk -- Asterisk	Unspecified vulnerability in the IAX2 channel driver (chan_iax2) for Asterisk 1.2.x before 1.2.9 and 1.0.x before 1.0.11 allows remote attackers to cause a denial of service (crash) via unknown vectors.	unknown 2006-06-07	2.3	CVE-2006-2898 BUGTRAQ BID OTHER-REF FRSIRT SECUNIA
CodeAvalanche -- CodeAvalanche FreeForum	Multiple cross-site scripting (XSS) vulnerabilities in post.asp in CodeAvalanche FreeForum (aka CAForum) 1.0 allow remote attackers to inject arbitrary web script or HTML via the (1) msg_subject and (2) msg_body parameters. NOTE: The provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-06-09	2.3	CVE-2006-2927 FRSIRT SECUNIA
D-Link -- DWL-2100AP	The web server for D-Link Wireless Access-Point (DWL-2100ap) firmware 2.10na and earlier allows remote attackers to obtain sensitive system information via a request to an arbitrary .cfg file, which returns configuration information including passwords.	2006-02-11 2006-06-07	2.3	CVE-2006-2901 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA
Drupal -- Drupal	Cross-site scripting (XSS) vulnerability in the upload module (upload.module) in Drupal 4.6.x before 4.6.8 and 4.7.x before 4.7.2 allows remote attackers to inject arbitrary web script or HTML via the uploaded filename.	unknown 2006-06-05	1.9	CVE-2006-2832 BUGTRAQ OTHER-REF OTHER-REF BID
Drupal -- Drupal	Cross-site scripting (XSS) vulnerability in the taxonomy module in Drupal 4.6.8 and 4.7.2 allows remote attackers to inject arbitrary web script or HTML via inputs that are not properly validated when the page title is output, possibly involving the $names variable.	unknown 2006-06-05	1.9	CVE-2006-2833 BUGTRAQ OTHER-REF OTHER-REF BID FRSIRT SECUNIA
Enigma Haber -- Enigma Haber	Cross-site scripting (XSS) vulnerability in hava.asp in Enigma Haber 4.2 allows remote attackers to inject arbitrary web script or HTML via the il parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-06-06	2.3	CVE-2006-2873 OTHER-REF BID
FunkBoard -- FunkBoard	profile.php in FunkBoard CF0.71 allows remote attackers to change arbitrary passwords via a modified uid hidden form field in an Edit Profile action.	unknown 2006-06-07	2.3	CVE-2006-2896 BUGTRAQ OTHER-REF FRSIRT SECUNIA
Funkboard -- Funkboard	Cross-site scripting (XSS) vulnerability in FunkBoard 0.71 allows remote attackers to inject arbitrary HTML or web script via unspecified vectors.	unknown 2006-06-07	1.9	CVE-2006-2897 FUNKBOARD FRSIRT SECUNIA

GANTTy -- GANTTy	Cross-site scripting (XSS) vulnerability in index.php in GANTTy 1.0.3 allows remote attackers to inject arbitrary HTML and web script via the message parameter in a login action.	unknown 2006-06-07	2.3	CVE-2006-2892 BUGTRAQ BID SECUNIA
GANTTy -- GANTTy	index.php in GANTTy 1.0.3 allows remote attackers to obtain the full path of the web server via an invalid lang parameter in an authenticate action.	unknown 2006-06-07	2.3	CVE-2006-2893 BUGTRAQ BID SECUNIA
GNOME -- GDM	GNOME GDM 2.8, 2.12, 2.14, and 2.15, when the "face browser" feature is enabled, allows local users to access the "Configure Login Manager" functionality using their own password instead of the root password, which can be leveraged to gain additional privileges.	unknown 2006-06-09	3.9	CVE-2006-2452 BUGTRAQ OTHER-REF BID
id Software -- Quake 3 Engine	Stack-based buffer overflow in the CL_ParseDownload function of Quake 3 Engine 1.32c and earlier, as used in multiple products, allows remote attackers to execute arbitrary code via a svc_download command with compressed data that triggers the overflow during expansion.	unknown 2006-06-06	2.3	CVE-2006-2875 OTHER-REF FRSIRT SECUNIA BUGTRAQ BID SECTRACK
Ingate -- Ingate Firewall Ingate -- Ingate SIParator	Ingate Firewall in the SIP module before 4.4.1 and SIParator before 4.4.1, when TLS is enabled or when SSL/TLS is enabled in the web server, allows remote attackers to cause a denial of service (crash) via a crafted SSL/TLS handshake.	unknown 2006-06-09	2.3	CVE-2006-2924 OTHER-REF SECUNIA
Ingate -- Ingate Firewall Ingate -- SIParator	Cross-site scripting (XSS) vulnerability in the web interface in Ingate Firewall before 4.4.1 and SIParator before 4.4.1 allows remote attackers to inject arbitrary web script or HTML, and steal cookies, via unspecified vectors related to "XSS exploits" in administrator functionality.	unknown 2006-06-09	3.7	CVE-2006-2925 OTHER-REF SECUNIA
Intelligent Solutions -- ASP Discussion Forum	Cross-site scripting (XSS) vulnerability in forum_search.asp in Intelligent Solutions Inc. ASP Discussion Forum allows remote attackers to inject arbitrary web script or HTML via the search variable.	unknown 2006-06-06	2.3	CVE-2006-2870 OTHER-REF BID FRSIRT SECUNIA
Jam Warehouse -- KnowledgeTree Open Source	view.php in KnowledgeTree Open Source 3.0.3 and earlier allows remote attackers to obtain the full installation path via a crafted fDocumentId parameter, which displays the path in the resulting error message. NOTE: this might be resultant from another vulnerability, since this vector also produces XSS.	2006-06-06 2006-06-07	2.3	CVE-2006-2886 OTHER-REF
MediaWiki -- MediaWiki	Cross-site scripting (XSS) vulnerability in MediaWiki 1.6.0 up to versions before 1.6.7 allows remote attackers to inject arbitrary HTML and web script via the edit form.	unknown 2006-06-07	1.9	CVE-2006-2895 MLIST OTHER-REF FRSIRT SECUNIA
Microsoft -- Internet Explorer	Internet Explorer 6 allows user-complicit remote attackers to read arbitrary files by tricking a user into typing the characters of the target filename in a text box and using the OnKeyDown, OnKeyPress, and OnKeyUp Javascript keystroke events to change the focus and cause those characters to be inserted into a file upload input control, which can then upload the file when the user submits the form.	unknown 2006-06-07	3.7	CVE-2006-2900 FULLDISC FRSIRT SECUNIA
Microsoft -- NetMeeting	Unspecified vulnerability in Microsoft NetMeeting 3.01 allows remote attackers to cause a denial of service (crash or CPU consumption) and possibly execute arbitrary code via crafted inputs that trigger memory corruption.	unknown 2006-06-08	3.3	CVE-2006-2919 BUGTRAQ OTHER-REF BID SECUNIA
Mozilla -- SeaMonkey Mozilla -- Firefox Netscape -- Netscape Mozilla -- Mozilla Suite	Mozilla Firefox 1.5.0.4, Mozilla Suite 1.7.13, Mozilla SeaMonkey 1.0.2, and Netscape 8.1 and earlier allows user-complicit remote attackers to read arbitrary files by tricking a user into typing the characters of the target filename in a text box and using the OnKeyDown, OnKeyPress, and OnKeyUp Javascript keystroke events to change the focus and cause those characters to be inserted into a file upload input control, which can then upload the file when the user submits the form.	unknown 2006-06-07	3.7	CVE-2006-2894 FULLDISC FRSIRT FRSIRT FRSIRT FRSIRT SECUNIA SECUNIA SECUNIA SECUNIA
OSADS Alliance Database -- OSADS Alliance Database	Unspecified vulnerability in OSADS Alliance Database before 1.4 has unknown impact and attack vectors related to a "Security Leak to lock in HTML-Code," possibly due to a cross-site scripting (XSS) vulnerability involving comments.	unknown 2006-06-06	2.3	CVE-2006-2874 OTHER-REF BID SECUNIA OTHER-REF FRSIRT

Out of the Trees Web Design -- SelectaPix	Cross-site scripting (XSS) vulnerability in SelectaPix 1.31 allows remote attackers to inject arbitrary web script or HTML via the albumID parameter to (1) popup.php and (2) view_album.php.	2006-05-17 2006-06-09	1.9	CVE-2006-2913 OTHER-REF SECUNIA
Particle Soft -- Particle Links	Directory traversal vulnerability in Particle Links 1.2.2 might allow remote attackers to access arbitrary files via ".." sequences in an HTTP request. NOTE: it is not clear whether this issue is legitimate, as the original researcher seems unsure.	unknown 2006-06-08	2.3	CVE-2006-2902 BUGTRAQ
Particle Soft -- Particle Links	Cross-site scripting (XSS) vulnerability in admin.php in Particle Links 1.2.2 allows remote attackers to inject arbitrary web script or HTML via the username parameter.	unknown 2006-06-08	1.9	CVE-2006-2903 BUGTRAQ FRSIRT SECUNIA
Particle Soft -- Particle Links	Partial Links 1.2.2 allows remote attackers to obtain sensitive information via a direct request to (1) page_footer.php and (2) page_header.php, which displays the path in an error message.	unknown 2006-06-08	2.3	CVE-2006-2905 BUGTRAQ FRSIRT SECUNIA
Pixelpost -- Pixelpost	Cross-site scripting (XSS) vulnerability in admin/index.php for Pixelpost 1-5rc1-2 and earlier allows remote attackers to inject arbitrary HTML or web script via the loginmessage parameter.	unknown 2006-06-07	1.9	CVE-2006-2891 BUGTRAQ OTHER-REF
Snort Project -- Snort	The HTTP Inspect preprocessor (http_inspect) in Snort 2.4.0 through 2.4.4 allows remote attackers to bypass "uricontent" rules via a carriage return (\r) after the URL and before the HTTP declaration.	unknown 2006-06-02	2.3	CVE-2006-2769 MLIST DEMARC BID OSVDB SECTRACK BUGTRAQ OTHER-REF SECUNIA BUGTRAQ BUGTRAQ BUGTRAQ FRSIRT
Sylpheed-Claws -- Sylpheed-Claws	Sylpheed-Claws before 2.2.2 allows remote attackers to bypass the URI check functionality and makes it easier to conduct phishing attacks via a URI that begins with a space character.	unknown 2006-06-08	1.9	CVE-2006-2920 SOURCEFORGE FRSIRT SECUNIA
Techno Dreams -- Guest Book	Cross-site scripting (XSS) vulnerability in Techno Dreams Guest Book allows remote attackers to inject arbitrary web script or HTML via certain comment fields in the "Sign Our GuestBook" page, probably the x_Comments parameter to guestbookadd.asp.	unknown 2006-06-06	2.3	CVE-2006-2837 OTHER-REF FRSIRT SECUNIA
Thomas Boutell -- graphics draw library	The LZW decoding in the gdImageCreateFromGifPtr function in the Thomas Boutell graphics draw (GD) library (aka libgd) 2.0.33 allows remote attackers to cause a denial of service (CPU consumption) via malformed GIF data that causes an infinite loop.	unknown 2006-06-08	2.7	CVE-2006-2906 BUGTRAQ BID FRSIRT SECUNIA
Tibco -- Runtime Agent Tibco -- Hawk Tibco -- Rendezvous	Buffer overflow in TIBCO Rendezvous before 7.5.1, TIBCO Runtime Agent (TRA) before 5.4, and Hawk before 4.6.1 allows remote attackers to cause a denial of service and possibly execute arbitrary code via the HTTP administrative interface.	2006-06-05 2006-06-05	2.3	CVE-2006-2830 OTHER-REF CERT-VN BID FRSIRT SECTRACK SECUNIA
WeBWorK -- WeBWorK	Directory traversal vulnerability in PG Problem Editor module (PGProblemEditor.pm) in WeBWorK Online Homework Delivery System 2.2.0 and earlier allows remote attackers to read and write files outside of the templates directory.	unknown 2006-06-06	2.3	CVE-2006-2839 OTHER-REF OTHER-REF FRSIRT SECUNIA

Back to top